

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
(zároveň ako Príloha č. 18 k Rámcovej dohode)

Číslo zmluvy:

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších
predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení
niektorých zákonov v znení neskorších predpisov
(ďalej len „**Zmluva KB**“)

medzi zmluvnými stranami:

Obchodné meno: **Národná diaľničná spoločnosť, a.s.**
Sídlo: Dúbravská cesta 14, 841 04 Bratislava, Slovenská republika
IČO: 35 919 001
DIČ: 2021937775
IČ DPH: SK2021937775
Zápis: oddelením Obchodného registra vedeného Mestským súdom Bratislava
III v Odd.: Sa, vložke č.: 3518/B
Zastúpenie: Ing. Filip Macháček, predseda predstavenstva a generálny riaditeľ, a
PhDr. Rastislav Droppa, podpredseda predstavenstva

(ďalej len „**Prevádzkovateľ kritickej základnej služby**“ alebo aj „**NDS**“)

a

Poskytovateľ/Zhotoviteľ:
Sídlo:
IČO:
IČ DPH:
Zastúpený:
Zapísaný:

(ďalej len „**Poskytovateľ/Zhotoviteľ**“)

(Prevádzkovateľ kritickej základnej služby a Poskytovateľ/Zhotoviteľ spolu ďalej len „**zmluvné strany**“)

Článok I.
ÚVODNÉ USTANOVENIA

1. **Národná diaľničná spoločnosť, a. s.** je podľa § 3 písm. m) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**ZoKB**“) prevádzkovateľom kritickej základnej služby Centrálny riadiaci systém tunela a Informačný systém diaľnic a rýchlostných ciest podľa § 3 ods. 2 zákona o kybernetickej bezpečnosti. Dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom služieb, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako Prevádzkovateľa kritickej základnej služby.
2. Poskytovateľ/Zhotoviteľ uzatvára s Prevádzkovateľom kritickej základnej služby „.....“ (ďalej len „**hlavná zmluva**“), ktorej predmet má vplyv na prevádzku, alebo priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v ZoKB pre

Prevádzkovateľa kritickej základnej služby (ďalej aj ako „**hlavný zmluvný vzťah**“). Konkrétny rozsah činností Poskytovateľa/Zhotoviteľa je identifikovaný v hlavnej zmluve.

3. Plnenie povinností podľa tejto Zmluvy KB sa vyžaduje počas celej doby trvania hlavného zmluvného vzťahu medzi Poskytovateľom/Zhotoviteľom a Prevádzkovateľom kritickej základnej služby, pričom táto Zmluva KB trvá najneskôr dovtedy, pokiaľ bude trvať hlavný zmluvný vzťah medzi Poskytovateľom/Zhotoviteľom a Prevádzkovateľom kritickej základnej služby.
4. V súlade s ustanovením § 19 ods. 2 ZoKB je Prevádzkovateľ kritickej základnej služby povinný pri uzatvorení zmluvy s Poskytovateľom/Zhotoviteľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Prevádzkovateľa kritickej základnej služby uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti hlavnej zmluvy.

Čl. II

Bezpečnostné opatrenia v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti

1. Poskytovateľ sa zaväzuje zachovávať mlčanlivosť o skutočnostiach zistených pri zabezpečení predmetu zákazky a poučiť svojich zamestnancov a spolupracujúce osoby o povinnosti zachovávať mlčanlivosť v zmysle platných zákonov, predovšetkým v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov. Mlčanlivosť sa vzťahuje na všetkých zamestnancov Poskytovateľa, ktorí prídu pri výkone svojej práce do styku s citlivými údajmi NDS a to najmä v pozíciách administrátora, programátora a pracovníka podpory. Títo zamestnanci majú záväzok mlčanlivosti zahrnutý v pracovnej zmluve a tento platí aj po ukončení pracovného pomeru s Poskytovateľom. Zoznam týchto zamestnancov bude poskytnutý NDS.
2. Poskytovateľ/Zhotoviteľ je povinný dodržiavať bezpečnostné politiky Prevádzkovateľa kritickej základnej služby, ktorých nevyhnutný obsah je prenesený do Prílohy č. 2 tejto Zmluvy KB, ktoré sa týkajú poskytovania služby podľa hlavnej zmluvy a poskytovania služby podľa hlavnej zmluvy, s ktorými ho Prevádzkovateľ kritickej základnej služby preukázateľne, formou poskytnutia Prílohy č. 2 tejto Zmluvy oboznámil, a to v rozsahu v akom súvisia s prevádzkovaním základnej služby Prevádzkovateľom kritickej základnej služby, a zároveň v akom ich je možné aplikovať na služby v zmysle predmetu hlavnej zmluvy.
3. Poskytovateľ sa zaväzuje dodržiavať bezpečnostné opatrenia v zmysle článku 2 tejto zmluvy a prílohy č. 2 tejto zmluvy a podriaďiť sa im.
4. Poskytovateľ je ďalej povinný doručiť zoznam pracovných rolí, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa, s povinnosťou oznámiť NDS každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti. NDS určí kontaktnú osobu pre komunikáciu s Poskytovateľom v oblasti technického zabezpečenia a kontaktnú osobu pre riešenie kybernetických incidentov.

Článok III.

ZODPOVEDNOSŤ ZA ŠKODU

1. Zmluvná strana zodpovedá za škodu preukázateľne a výlučne spôsobenú zavineným porušením povinností zmluvnej strany stanovenej ZoKB, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvou KB.
2. V prípade, ak v dôsledku porušenia ZoKB alebo preukázateľného porušenia povinností vyplývajúcich z tejto Zmluvy KB na strane Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov vznikne Prevádzkovateľovi kritickej základnej služby ujma alebo finančná sankcia, Poskytovateľ/Zhotoviteľ zodpovedá za spôsobenú škodu podľa ustanovení ZoKB. V prípade sankcie uloženej Národným bezpečnostným úradom, túto znáša v plnom rozsahu Poskytovateľ/Zhotoviteľ.

3. V prípade, že zmluvná strana poruší svoju povinnosť, ktorá jej vyplýva zo ZoKB, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvy KB (ďalej ako „**porušujúca zmluvná strana**“) a v dôsledku tohto konania alebo opomenutia konania porušujúcej zmluvnej strany preukázateľne dôjde k vzniku škody na strane druhej zmluvnej strany (ďalej ako „**poškodená zmluvná strana**“), zaväzuje sa porušujúca zmluvná strana túto škodu vzniknutú poškodenej zmluvnej strane nahradiť.
4. Vznik zodpovednosti porušujúcej zmluvnej strany za škodu vzniknutú poškodenej zmluvnej strane je však podmienená povinnosťou poškodenej zmluvnej strany preukázať porušujúcej zmluvnej strane existenciu príčinnej súvislosti medzi porušením povinnosti podľa Zmluvy KB alebo ZoKB, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy na strane porušujúcej zmluvnej strany a vznikom škody. Príčinná súvislosť je okrem iného daná aj vtedy, ak porušujúca zmluvná strana nesplnila svoju všeobecnú preventívnu povinnosť počínať si tak, aby nedochádzalo ku vzniku škôd. Počínaním podľa predchádzajúcej vety sa rozumie najmä akýkoľvek postup zmluvnej strany, na ktorý je v zmysle Zmluvy KB alebo ZoKB, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy oprávnená a prostredníctvom ktorého mohlo byť vzniku škody zabránené.
5. V prípade preukázania existencie príčinnej súvislosti podľa tohto článku Zmluvy KB je porušujúca zmluvná strana povinná uhradiť poškodenej zmluvnej strane vzniknutú škodu, a to v lehote do 10 (desať) dní odo dňa doručenia písomnej výzvy porušujúcej zmluvnej strane na adresu uvedenú v záhlaví tejto Zmluvy KB. V prípade potreby vzniknutú škodu posúdi nezávislá tretia strana, ktorú zabezpečí Prevádzkovateľ kritickej základnej služby.
6. Zánikom tejto Zmluvy KB nie sú dotknuté tie ustanovenia, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zániku tejto Zmluvy KB a záväzky na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy KB.

Článok IV.

KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

1. Poskytovateľ/Zhotoviteľ sa zaväzuje komunikovať pri plnení povinností podľa tejto Zmluvy KB s Prevádzkovateľom kritickej základnej služby spôsobom určeným Prevádzkovateľom kritickej základnej služby, t.j. v zmysle komunikačnej matice – príloha č. 4 tejto Zmluvy, pričom Poskytovateľ/Zhotoviteľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií (napr. PGP šifrovanie).
2. Prevádzkovateľ kritickej základnej služby a Poskytovateľ/Zhotoviteľ určuje kontaktné osoby pre komunikáciu s Poskytovateľom/Zhotoviteľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy KB.
3. Kontaktné osoby podľa prílohy č. 1 tejto Zmluvy KB môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve KB. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia Zmluvy KB o doručovaní.

Článok V.

SPOLOČNÉ USTANOVENIA

1. Poskytovateľ/Zhotoviteľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy KB v súlade so ZoKB a jeho vykonávacími predpismi ostatnej platnej legislatívy, vrátane všeobecných bezpečnostných opatrení, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných

incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

2. Poskytovateľ/Zhotoviteľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa kritickej základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa kritickej základnej služby tak, aby nebola narušená ich dostupnosť, dôverynosť, autentickosť a integrita.
3. Poskytovateľ/Zhotoviteľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto Zmluvy KB na zabezpečenom priestore tak, aby nebola narušená ich dôverynosť, autentickosť a integrita.
4. Poskytovateľ/Zhotoviteľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy KB bezodkladne od účinnosti hlavnej zmluvy a odo dňa prebratia diela k plneniu predmetu hlavnej zmluvy, pokiaľ to nie je v tejto Zmluve KB alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.
5. Poskytovateľ/Zhotoviteľ, prípadne jeho subdodávateľ zabezpečujúci príslušné činnosti, vyhlasuje, že disponuje so všetkým potrebným technickým, technologickým a personálnym vybavením, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto Zmluvy KB, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto Zmluvy KB pre identifikáciu prípadne pre opravu poruchy/incidentu a zabezpečenie bezpečnej prevádzky IS.
6. V prípade, ak Poskytovateľ/Zhotoviteľ plní Zmluvu KB prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa kritickej základnej služby, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa kritickej základnej služby, Poskytovateľ/Zhotoviteľ sa zaväzuje zabezpečiť plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tejto Zmluvy KB aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto Zmluvy KB. Poskytovateľ/Zhotoviteľ sa zaväzuje zabezpečiť, aby Prevádzkovateľ kritickej základnej služby mohol vykonať kontrolný audit v súlade s ustanoveniami tejto Zmluvy KB aj u týchto subdodávateľov.
7. Akékoľvek oznámenia zmluvných strán podľa tejto Zmluvy KB realizované formou e-mailu sa považujú za doručené druhej zmluvnej strane nasledujúci pracovný deň po dni, kedy bolo odosielateľovi preukázateľne odoslané potvrdenie o doručení e-mailu adresátovi bez ohľadu na to, či došlo k prečítaniu správy na strane adresáta, s tým, že v prípade detekcie kybernetického bezpečnostného incidentu a povinností Poskytovateľa/Zhotoviteľa spojených s jeho hlásením Prevádzkovateľovi kritickej základnej služby sa zaväzuje komunikovať podľa tejto Zmluvy KB spôsobom určeným Prevádzkovateľom kritickej základnej služby, t.j. v zmysle komunikačnej matice.
8. Prevádzkovateľ kritickej základnej služby je oprávnený vykonať na dotknutom diele, v rámci ktorého sa nachádza kritická základná služba Prevádzkovateľa kritickej základnej služby voči Poskytovateľovi/Zhotoviteľovi ako aj u jeho subdodávateľov audit zameraný na overenie plnenia povinností Poskytovateľa/Zhotoviteľa a subdodávateľov podľa tejto Zmluvy KB a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Poskytovateľa/Zhotoviteľa a subdodávateľov na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Poskytovateľa/Zhotoviteľa a subdodávateľov pre plnenie cieľov tejto Zmluvy KB.
9. Prípadné nedostatky zistené auditom sú Poskytovateľom/Zhotoviteľom a subdodávateľmi povinní odstrániť bez zbytočného odkladu. V prípade, že tieto nedostatky nebudú v lehote 60

(šesťdesiat) dní od zistenia na základe auditu odstránené, považuje sa to za podstatné porušenie Zmluvy KB zo strany Poskytovateľa/Zhotoviteľa.

10. Prevádzkovateľ kritickej základnej služby môže audit voči Poskytovateľovi/Zhotoviteľovi a subdodávateľom realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa kritickej základnej služby pri výkone auditu realizuje Prevádzkovateľom základnej služby poverená tretia osoba.
11. Poskytovateľ/Zhotoviteľ sa zaväzuje za seba ako aj za subdodávateľov pri audite spolupracovať s Prevádzkovateľom základnej služby, príp. s poverenou treťou osobou a sprístupniť mu priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB a hlavnou zmluvou, prípadne poskytnúť ďalšiu potrebnú súčinnosť.
12. Prevádzkovateľ kritickej základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom Poskytovateľa/Zhotoviteľa a subdodávateľom, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti a prevádzky systémov podľa hlavnej zmluvy a tejto Zmluvy KB.
13. V rámci auditu sú Poskytovateľ/Zhotoviteľ a subdodávatelia povinní preukázať Prevádzkovateľovi kritickej základnej služby súlad s touto Zmluvou KB, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzkov a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto Zmluvy KB a aktuálnosť svojej bezpečnostnej dokumentácie.
14. Prevádzkovateľ kritickej základnej služby sa zaväzuje oznámiť Poskytovateľovi/Zhotoviteľovi najmenej 15 (pätnásť) pracovných dní vopred svoj zámer realizovať u Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov audit. Vykonanie alebo nevykonanie auditu Prevádzkovateľom základnej služby nezavahuje Zhotoviteľa zodpovednosti za plnenie povinností Poskytovateľa/Zhotoviteľa vyplývajúcich z tejto Zmluvy KB. Ak Zhotoviteľ alebo jeho subdodávateľ neumožní vykonanie auditu, považuje sa to za podstatné porušenie Zmluvy KB a Prevádzkovateľ kritickej základnej služby je oprávnený vyvodiť voči Poskytovateľovi/Zhotoviteľovi zmluvné sankcie.
15. Poskytovateľ/Zhotoviteľ sa zaväzuje písomne informovať Prevádzkovateľa kritickej základnej služby v zmysle komunikačnej matice o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Zhotoviteľom.
16. Prevádzkovateľ kritickej základnej služby ako aj Poskytovateľ/Zhotoviteľ sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia článku VII. ods. 2, 3 a 4 tejto Zmluvy KB sa uplatňujú primerane.
17. Prevádzkovateľ kritickej základnej služby a jeho zamestnanci pri návšteve priestorov Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov v rámci výkonu auditu musia dodržiavať pokyny Zhotoviteľa alebo jeho subdodávateľov týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „**BOZP**“) a ochrany pred požiarom na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „**PO**“), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ kritickej základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Zhotoviteľ. Zhotoviteľ sa zaväzuje pred vykonaním auditu v priestoroch Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov písomne informovať zamestnancov Prevádzkovateľa kritickej základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Poskytovateľa/Zhotoviteľa alebo jeho subdodávateľov môžu vyskytnúť a o výsledkoch

posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Poskytovateľ/Zhotoviteľ alebo jeho subdodávateľa na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia, vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Zhotoviteľa alebo jeho subdodávateľov.

18. Pre vylúčenie akýchkoľvek pochybností sa Poskytovateľ/Zhotoviteľ zaväzuje zabezpečiť Prevádzkovateľovi kritickej základnej služby vykonanie auditu v zmysle tohto článku tejto Zmluvy KB aj u svojich subdodávateľov.
19. Poskytovateľ/Zhotoviteľ je počas trvania zmluvného vzťahu povinný vykonávať a realizovať bezpečnostné opatrenia v súlade s touto písomnou zmluvou a zákonom o kybernetickej bezpečnosti a je povinný podrobiť sa kontrole plnenia týchto opatrení zo strany Prevádzkovateľa kritickej základnej služby v zmysle ods. 2 § 19 zákona o kybernetickej bezpečnosti. Ak ide o zmluvu uzatvorenú s iným Prevádzkovateľom kritickej základnej služby, ktorý prevádzkuje kritickú základnú službu, kontrolu môže vykonávať aj Národný bezpečnostný úrad (ďalej len „NBÚ“); na tento účel má Poskytovateľ/Zhotoviteľ, t.j. tretia strana postavenie Prevádzkovateľa kritickej základnej služby.
20. Prevádzkovateľ kritickej základnej služby je oprávnený, na základe identifikácie skutočností vyplývajúcich z analýzy rizík, určiť, že Poskytovateľ/Zhotoviteľ má významný vplyv na zabezpečenie kybernetickej bezpečnosti kritickej základnej služby.
21. V prípade, že analýza rizík Prevádzkovateľa kritickej základnej služby potvrdí významný vplyv Poskytovateľa/Zhotoviteľa na zabezpečenie kybernetickej bezpečnosti kritickej základnej služby, Prevádzkovateľa kritickej základnej služby je povinný túto skutočnosť nahlásiť NBÚ.
22. NBÚ následne podnet posúdi a v súlade s § 17 ods. 1 písm. i) a ods. 3 ZoKB Poskytovateľa/Zhotoviteľa zaradí do registra prevádzkovateľov základnej služby.
23. Zhotoviteľ je povinný poskytnúť Prevádzkovateľovi všetku potrebnú súčinnosť pri plnení povinností vyplývajúcich z tohto článku.

Článok VI.

VYŠŠIA MOC

1. Vyššia moc znamená mimoriadnu udalosť alebo okolnosť, ktorú nemohla žiadna zo zmluvných strán pred uzatvorením Zmluvy KB predvídať, ktorá je mimo kontroly ktorejkoľvek zo zmluvných strán a nebola spôsobená úmyselne alebo z nedbanlivosti konaním alebo opomenutím ktorejkoľvek zmluvnej strany a ktorá podstatným spôsobom sťažuje alebo znemožňuje plnenie povinností podľa Zmluvy KB ktoroukoľvek zo zmluvných strán. Takýmito udalosťami alebo okolnosťami sú najmä živelné pohromy alebo prírodné katastrofy. Výslovne sa stanovuje, že vyššou mocou nie je štrajk personálu Poskytovateľa/Zhotoviteľa ani hospodárske pomery zmluvných strán.
2. Ak niekto zmluvných strán bráni alebo bude brániť v plnení niektorej jej povinnosti podľa Zmluvy KB vyššia moc, potom písomne oznámi druhej zmluvnej strane udalosť alebo okolnosť, ktoré predstavujú vyššiu moc, uvedie povinnosti, v ktorých plnení jej vyššia moc bráni alebo bude brániť a predpokladané trvanie takej okolnosti predstavujúcej vyššiu moc. Oznámenie musí byť urobené bezodkladne, najneskôr však v lehote 15 (pätnásť) dní potom, čo sa zmluvná strana dozvedela alebo sa pri vynaložení riadnej odbornej starostlivosti mala a mohla dozvedieť o

príslušnej udalosti alebo okolnostiach predstavujúcich dôvod vyššej moci. Ak je to možné, pri vynaložení riadnej odbornej starostlivosti, musí uvedené oznámenie obsahovať návrh opatrení vedúcich k zmierneniu alebo vylúčeniu dôsledkov okolností predstavujúcich vyššiu moc. V ostatných prípadoch bude oznámenie obsahovať iba najbližší možný termín, do ktorého môže byť návrh opatrenia poskytnutý pri vynaložení primeraného úsilia. Ak návrh opatrenia druhá zmluvná strana schváli, na čo má lehotu 15 (pätnásť) dní, postupuje zmluvná strana dotknutá vyššou mocou podľa neho až do ukončenia okolností vyššej moci.

3. Po uskutočnení tohto oznámenia príslušnou zmluvnou stranou, nebude táto zmluvná strana zodpovedná za príslušné porušenia povinností po dobu, dokiaľ jej vyššia moc bráni alebo bude brániť v ich plnení.
4. Zmluvnú stranu nezbavuje zodpovednosti za porušenie povinnosti vyššia moc, ktorá nastala až v čase, kedy bola povinná zmluvná strana v omeškaní s plnením jej povinnosti. Účinky vylúčenia zodpovednosti sú obmedzené iba na dobu, dokiaľ trvá vyššia moc.
5. Každá zmluvná strana vždy vyvinie všetko úsilie potrebné k tomu, aby minimalizovala omeškanie pri plnení svojich povinností podľa Zmluvy KB, ktoré vzniklo v dôsledku vyššej moci, najmä plniť návrh opatrenia, ak je tento schválený druhou zmluvnou stranou.
6. Príslušná zmluvná strana oznámi druhej zmluvnej strane okamih ukončenia pôsobenia vyššej moci v rovnakej lehote ako pri oznámení o jej vzniku podľa bodu 2 tohto článku tejto Zmluvy KB.
7. Ak je z dôvodu okolnosti vylučujúcej zodpovednosť alebo prípadu vyššej moci plnenie Zmluvy KB jednej zo zmluvných strán ovplyvnené len čiastočne, takáto zmluvná strana zostáva zodpovedná za plnenie tých záväzkov, ktoré okolnosťou vylučujúcou zodpovednosť alebo vyššou mocou nie sú dotknuté.
8. Ak má niektorý zo subdodávateľov podľa akejkoľvek zmluvy či dohody týkajúcej sa poskytovania služby podľa tejto Zmluvy KB širšie definovaný nárok na omeškanie v dôsledku pôsobenia vyššej moci, okolností vylučujúcich zodpovednosť alebo iného obdobného právneho inštitútu, než ako je definovaná vyššia moc podľa tejto Zmluvy KB, takáto širšie definovaná udalosť alebo okolnosť neospravedlňuje porušenie povinností podľa Zmluvy KB s Poskytovateľom/Zhotoviteľom ani mu nezakladajú nároky podľa tohto článku Zmluvy KB.

Článok VII. SANKCIE

1. Zmluvné strany sa dohodli, že v prípade porušenia ktorejkoľvek povinnosti Poskytovateľa uvedenej v bode 1 až 7 prílohy č. 2 tejto Zmluvy je Objednávateľ oprávnený uložiť Poskytovateľovi zmluvnú pokutu vo výške 500 EUR (slovom: päťsto eur) za každý, aj začiatí deň trvania porušenia povinnosti, až do vykonania nápravy, a to aj opakovane a za každé jednotlivé porušenie povinnosti samostatne.
2. V prípade, ak Poskytovateľ/Zhotoviteľ spôsobí Prevádzkovateľovi kritickej základnej služby porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo Zmluvy KB akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. Obchodného zákonníka. Pre odstránenie právnych pochybností, zodpovednosť Poskytovateľa/Zhotoviteľa nevyklučuje prekážka, ktorá vznikla až v čase, keď bol Poskytovateľ/Zhotoviteľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Prevádzkovateľovi kritickej základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Poskytovateľom/Zhotoviteľom.

3. Zmluvné strany sa dohodli, že uplatnením sankcií v zmysle tohto článku Zmluvy KB nie je dotknutý nárok Prevádzkovateľa kritickej základnej služby na náhradu škody, ktorá mu vznikla porušením povinností Poskytovateľa/Zhotoviteľa.
4. Zaplatenie zmluvnej pokuty nezavahuje Poskytovateľa/Zhotoviteľa povinnosti splniť záväzok zabezpečený zmluvnou pokutou.

Článok VIII. TRVANIE ZMLUVY

1. Táto Zmluva KB sa uzatvára na dobu určitú, a to na dobu trvania hlavnej zmluvy.
2. Za podstatné porušenie Zmluvy KB sa považuje:
 - a) porušenie ktorejkoľvek povinnosti uvedenej v tejto Zmluve KB;
 - b) ak Poskytovateľ/Zhotoviteľ, ako strana porušujúca Zmluvu KB, vedel v čase uzavretia Zmluvy KB alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel Zmluvy KB, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola Zmluva KB uzavretá, že Prevádzkovateľ kritickej základnej služby nebude mať záujem na plnení povinností pri takom porušení Zmluvy KB;
 - c) Poskytovateľ/Zhotoviteľ neposkytne potrebnú súčinnosť v zmysle tejto Zmluvy KB.
3. Odstúpením/okamžitým odstúpením od hlavnej zmluvy Zmluva KB zaniká.
4. Túto Zmluvu KB nie je možné vypovedať Poskytovateľom/Zhotoviteľom ani Prevádzkovateľom kritickej základnej služby, a je viazaná na účinnosť hlavnej zmluvy.
5. Po zániku tejto Zmluvy KB je Poskytovateľ/Zhotoviteľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa kritickej základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Prevádzkovateľom kritickej základnej služby. Licenčné podmienky sa riadia hlavnou zmluvou. .

Článok IX. ZÁVEREČNÉ USTANOVENIA

1. Táto Zmluva KB sa spravuje zákonmi Slovenskej republiky. Právne vzťahy výslovne neupravené touto zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.
2. Prípadné spory vyplývajúce z tejto Zmluvy KB budú riešené predovšetkým mimosúdne. Podpisom tejto Zmluvy KB zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto Zmluvy KB sú príslušné súdy Slovenskej republiky.
3. Táto Zmluva KB sa môže meniť, dopĺňať iba dohodou zmluvných strán v písomnej forme, ak zo Zmluvy KB nevyplýva niečo iné.
4. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto Zmluvy KB na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.
5. V prípade, ak niektoré z ustanovení Zmluvy KB je alebo sa stane neúplným, neplatným, neúčinným a/alebo nevykonateľným, nie sú tým dotknuté ostatné ustanovenia Zmluvy KB, pokiaľ z jeho povahy, obsahu alebo okolností, za ktorých bolo dojednané nevyplýva, že ho nie je možné oddeliť od ostatného obsahu Zmluvy KB. Zmluvné strany sa zaväzujú bez zbytočného odkladu nahradiť takéto neúplné, neplatné, neúčinné a/alebo nevykonateľné ustanovenie, takým úplným, platným, účinným a/alebo vykonateľným ustanovením, ktoré svojím obsahom najviac zodpovedá nahrádzanému ustanoveniu.

6. Táto Zmluva KB predstavuje úplnú dohodu zmluvných strán o jej obsahu. Podpisom tejto Zmluvy KB zanikajú všetky predchádzajúce písomné a ústne zmluvy súvisiace s predmetom tejto Zmluvy KB a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych, v tejto Zmluve KB neuvedených, ústnych alebo písomných dojednaní a dohôd.
7. Táto Zmluva KB bola vyhotovená v **(4) štyroch** rovnopisoch, po (2) dvoch pre každú zmluvnú stranu.
8. Zmluvné strany berú na vedomie, že Prevádzkovateľ kritickej základnej služby je v zmysle § 2 ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov povinnou osobou, a preto je táto zmluva v zmysle § 5a tohto zákona v spojení s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov povinne zverejňovanou zmluvou.
9. Táto Zmluva KB nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv.
10. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
 - Príloha č. 1 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa kritickej základnej služby a Poskytovateľa/Zhotoviteľa, **(nezverejňuje sa v CRZ, GDPR)**
 - Príloha č. 2 - Špecifikácia a rozsah bezpečnostných opatrení (vyplývajúce z Bezpečnostných smerníc Prevádzkovateľa kritickej základnej služby),**(nezverejňuje sa v CRZ)**
 - Príloha č. 3 – Vzor - Záznam o kybernetickom bezpečnostnom incidente
11. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto Zmluvu KB neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah Zmluvy KB dôkladne prečítali, a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu a na znak súhlasu ju podpisujú.

Prevádzkovateľ kritickej základnej služby:

V Bratislave dňa.....

(obchodné meno)
(titul, meno, priezvisko
štatutára)
(funkcia)

Poskytovateľ/Zhotoviteľ:

V dňa

(obchodné meno)
(titul, meno, priezvisko
štatutára)
(funkcia)

Príloha č. 1: Zoznam pracovných rolí a kontaktov Prevádzkovateľa kritickej základnej služby a Poskytovateľa/Zhotoviteľa (**nezverejňuje sa v CRZ, GDPR**)

Prevádzkovateľ kritickej základnej služby:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email

Poskytovateľ/Zhotoviteľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email

Špecifikácia a rozsah bezpečnostných opatrení Plnením bezpečnostných opatreniami a všetkých činností v zmysle zákona č.69/2018 Z. z. o kybernetickej bezpečnosti sa rozumejú činnosti nad prostredím dotknutej prevádzkovej základnej služby, a nejedná sa o interné prostredie Poskytovateľa/Zhotoviteľa. Požadované plnenie politík a postupov, sa taktiež týka výhradne dotknutej prevádzkovej základnej služby.

1. Pre oblasť riadenia prístupov realizuje Poskytovateľ/Zhotoviteľ opatrenia podľa § 8 Vyhlášky NBÚ č. 362/2018, Z.z., prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

- a. dodržiavať zásady riadenia prístupu k informáciám NDS,
- b. riadenia prístupu používateľov v dotknutých systémoch;
- c. dodržiavanie a vymedzenie príslušných zodpovedností používateľov a rolí v dotknutých systémoch;
- d. riadenia prístupu k sieťam, čím sa rozumie:
 - i. že každému používateľovi siete a informačného systému sa prideliť jednoznačný identifikátor na autorizovaný vstup do siete a informačného systému;
 - ii. zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane ich prístupových práv;
 - iii. využívanie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroja na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy);
 - iv. na vyzvanie poskytnúť súčinnosť pre NDS pri výkone kontroly súladu schválených používateľských účtov a prístupových oprávnení v pravidelných intervaloch, najmenej však raz ročne, a to vo forme poskytnutia aktuálneho výpisu pridelených prístupových oprávnení do IS a podporných systémov a v prípade ich nesúladu následné bezodkladné deaktivovanie, resp. zmazanie;
 - v. určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za pridelenie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle bezpečnostnej stratégie alebo príslušnej bezpečnostnej politiky NDS. (Určenú zodpovednú osobu požaduje NDS aj na strane Poskytovateľa/Zhotoviteľa ako aj na strane NDS).
- e. riadenie prístupov osôb k sieti a informačnému systému je založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa.
- f. NDS požaduje:
 - i. Pridelovať a odoberať prístupy iba na základe požiadavky gestora prevádzkovej základnej služby, alebo ním určenej oprávnenej osoby,
 - ii. V prípade potreby poskytnutie súčinnosti pri aktualizácii Evidencie prístupov, ktorú vedie Poskytovateľ/Zhotoviteľ,
 - iii. Pri pridelení prístupov zástupcom Poskytovateľa/Zhotoviteľa dodržiavať princíp najnižšieho oprávnenia, a to aby používatelia mali prístup len k tým systémom a dátam, ktoré sú nevyhnutné pre ich pracovné úlohy,

- iv. Zabezpečiť logovanie aktivít, a to všetkých prístupov a aktivít používateľov v systéme,
- v. Zabezpečiť monitorovanie v reálnom čase, a to použitím nástroja na sledovanie a analýzu prístupových záznamov v reálnom čase.
- g. riadenie prístupov k sieťam a informačným systémom sa uskutočňuje v závislosti od prevádzkových a bezpečnostných potrieb Prevádzkovateľa kritickej základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabráňujú zneužitiu týchto údajov neoprávnenou osobou.
- h. musí byť využívaná funkcia zabezpečeného prístupu do systému formou protokolu mechanizmu AAA (Authentication-Authorization-Accounting),
- i. kópia hesiel k privilegovaným účtov (k účtom s najvyššími oprávneniami systémov) musí byť v čase prevádzky uložená v zabezpečenej schválenej forme MIKB NDS v zabezpečenom priestore Poskytovateľa/Zhotoviteľa. V prípade potreby prístupu k uvedeným heslám, musí byť o prístupe a ich použití informovaný MIKB NDS najneskôr do 48 hodín ,
- j. Poskytovateľ k dňu ukončenia hlavného zmluvného vzťahu zlikviduje všetky prístupy podľa zmluvy a všetky informácie, ktoré majú, alebo by mohli mať charakter dôverných informácií a na ktoré sa vzťahuje záväzok mlčanlivosti.
- k.

2. Pre oblasť technických zraniteľností systémov a zariadení realizuje Poskytovateľ/Zhotoviteľ opatrenia podľa § 11 Vyhlášky NBÚ č. 362/2018 Z.z., identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb pre NDS a ktoré toto poskytovanie služieb NDS ovplyvňujú, napríklad prostredníctvom opatrení definovaných v nasledujúcich bodoch alebo opatrení s porovnateľným účinkom:

- a) Implementácia nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí;
- b) Implementácia nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí;
- c) využívanie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov,
- d) Poskytovateľ/Zhotoviteľ je povinný vykonávať pravidelné bezpečnostné kontroly zamerané na detekciu existujúcich zraniteľností v sieťových aktívach. Tieto kontroly sa budú vykonávať minimálne raz ročne pre všetky sieťové aktíva a minimálne raz štvrtročne pre aktíva určené ako kritické. Kritické aktíva budú definované na základe ich dôležitosti pre prevádzku a bezpečnosť systému. V prípade identifikácie zraniteľností je Poskytovateľ/Zhotoviteľ povinný bezodkladne prijať primerané opatrenia na ich odstránenie alebo zmiernenie rizík.
- e) V prípade identifikácie zraniteľností s vyšším CVSS 3.0 ako hodnota 7.0, Poskytovateľ/Zhotoviteľ poskytne NDS zoznam týchto identifikovaných zraniteľností aj s určeným dotknutých aktív.
- f) Poskytovateľ/Zhotoviteľ zabezpečí identifikáciu potrieb softvérových záplat a aktualizácií, ako aj zabezpečuje ich implementáciu.
- g) Poskytovateľ/Zhotoviteľ vedie evidenciu softvérových záplat a aktualizácií a informácie o ich nasadení alebo o dôvodoch nenasadenia, a na požiadanie je povinný ju poskytnúť NDS. V prípade rozhodnutia Poskytovateľa/Zhotoviteľa nenasadiť bezpečnostnú záplatu alebo aktualizáciu je povinný Poskytovateľ/Zhotoviteľ informovať MIKB NDS o dôvodoch nenasadenia.
- h) Poskytovateľ/Zhotoviteľ je povinný testovať softvérové záplaty a aktualizácie pred ich nasadením do ostrej prevádzky systému,

- i) Poskytovateľ/Zhotoviteľ je povinný aktualizovať plány softvérových záplat a aktualizácií.

3. Pre oblasť ochrany proti škodlivému kódu, realizuje Poskytovateľ/Zhotoviteľ opatrenia podľa §12 Vyhlášky NBÚ č. 362/2018, Z.z., prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

- a) Inštalovať a aktualizovať antivírusový softvér na všetkých zariadeniach, ak to daná technológia umožňuje,
- b) Všetky oprávnené osoby s prístupom do systému (t. j. používateľov technológie) musia byť preškolení v rámci prevencie pred škodlivým kódom,
- c) Všetci používatelia sú povinní dodržiavať pravidlá alebo postupy, aby sa zabránilo vniknutiu škodlivého softvéru (ako sú vírusy, malware, trojany a podobne) do počítačových systémov.
- d) Je povolené vyberať len overené antivírusové a antimalware programy od renomovaných výrobcov.
- e) Poskytovateľ/Zhotoviteľ je povinný zabezpečiť, aby antivírusový a antimalware softvér (signatúry) bol vždy aktuálny.
- f) Poskytovateľ/Zhotoviteľ je povinný naplánovať a vykonávať pravidelné skenovanie systémov na detekciu škodlivého kódu minimálne raz štvrtročne.
- g) Poskytovateľ/Zhotoviteľ je povinný nastaviť systém na monitorovanie a automatické upozorňovanie na podozrivé aktivity alebo detegované hrozby.
- h) Poskytovateľ/Zhotoviteľ je povinný zabezpečiť monitorovanie potenciálnych ciest prieniku škodlivého kódu do prostredia sietí a informačných systémov prevádzkovanvej základnej služby.

4. Pre oblasť riadenia bezpečnosti sietí a informačných systémov realizuje Poskytovateľ/Zhotoviteľ opatrenia podľa §13 Vyhlášky NBÚ č. 362/2018, Z.z., prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

- a) riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov,
- b) prepojenia medzi segmentami a externými sieťami, musia byť chránené firewallom a všetky spojenia sú povoľované na princípe zásady najnižších privilégií,
- c) bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup (napr. bezpečným spôsobom s použitím dvojfaktorovej autentifikácie alebo použitím kryptografických prostriedkov); Vzdialený prístup Poskytovateľa/Zhotoviteľa a jeho subdodávateľov v zmysle zmluvy do IS musí byť schválený NDS v zmysle vopred definovaných postupov.
- d) V prípade mimoriadnej situácie, napr. zásah pri bezpečnostnom incidente, pri prevádzkovom incidente môže byť vzdialený prístup schválený dodatočne najneskôr nasledujúci pracovný deň.
- e) opatrenia, že spojenia z a do externých sietí sú smerované cez sieťový firewall a systém detekcie prienikov;
- f) serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu;
- g) udržiavania zoznamu všetkých vstupno-výstupných bodov na perimetri siete v aktuálnom stave a poskytnutia uvedeného zoznamu NDS minimálne raz ročne a na požiadanie; ;

- h) použitia automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou;
- i) blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje;
- j) zakázanie komunikácie a prevádzky aplikácií cez nevyužívané porty;
- k) systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na perimetri siete v zmysle požiadaviek bodu 5 tejto prílohy ;
- l) implementácie systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky formou IDS je povinné a v prípade technických možností bez vplyvu na funkciu informačných systémov sa požadujú aj IPS;
- m) použitia dvojfaktorovej autentizácie každého vzdialeného pripojenia do internej siete;
- n) vykonávania pravidelného posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti,
- o) dodržiavať postupy a nastavenie systémov v zmysle schválenej technickej špecifikácie dotknutých systémov.

5. Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Poskytovateľ/Zhotoviteľ opatrenia podľa § 15 Vyhlášky NBÚ č. 362/2018, Z.z. v rozsahu potrebnom pre poskytovanie služieb pre NDS.

Monitorovanie bezpečnosti sietí a informačných systémov sa uskutočňuje implementáciou centrálného nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho bezpečnostný dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu:

- a) sieťových prvkov a serverov, ktoré sú súčasťou predmetu zákazky,
- b) služieb prístupných do externých sietí, ak sú súčasťou predmetu zákazky.
- c) Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov musí vytvárať prevádzkové záznamy a zaznamenávať najmenej:
 - i) aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených,
 - ii) iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy,
 - iii) pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla,
 - iv) automatické varovné alebo chybové hlásenia systémov,
 - v) detegované podozrivé alebo škodlivé aktivity a
- d) ďalšie informácie nevyhnutné na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a korektné informácie o dátume, čase a použitej časovej zóne.

Prevádzkové záznamy musia byť zabezpečené, a to najmenej tak, že

- i) sú čitateľné výlučne osobám povereným ich analýzou,
- ii) zamedzujú možnosti prepísania alebo vymazania záznamu,

- iii) záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete,
- iv) sú uchovávané po dobu zodpovedajúcu kategórii informačného systému.

6. Pre oblasť riešenia KBI realizuje Poskytovateľ/Zhotoviteľ opatrenia podľa § 17 Vyhlášky NBÚ č. 362/2018, Z.z., najmä deteguje a rieši KBI, ktoré môžu mať dopad na poskytovanie služieb pre NDS. To zahŕňa napríklad prijatie opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

- a) oboznámenie sa s postupmi NDS pri riešení KBI a spracovanie interných postupov riešenia KBI, ktoré zahŕňajú minimálne postupy hlásenia KBI voči NDS.
- b) Zabezpečenie technických podmienok v zmysle písm. f ods. 5 tejto prílohy z dôvodu zabezpečenia plnenia zákonných povinností NDS s cieľom zabezpečiť monitorovanie a analyzovanie bezpečnostných udalostí v sieťach a informačných systémoch, a to zabezpečiť:
 - i) detegovanie KBI, prostredníctvom nástroja na detekciu KBI, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.
 - ii) zber a vyhodnocovanie relevantných informácií o KBI prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o KBI; za relevantné informácie NDS považuje informácie minimálne v rozsahu potrebnom na nahlásenie KBI na Národný bezpečnostný úrad.
 - iii) vyhľadávanie a zoskupovanie záznamov súvisiacich s KBI; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako KBI podľa pokynov NDS; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných KBI.
- c) NDS požaduje zabezpečiť rolu s prístupom Read Only do všetkých bezpečnostných nástrojov pre dotknutú základnú službu pre riešenie KBI a bezpečnosť siete,
- d) riešenie zistených KBI a zníženie následkov zistených KBI podľa postupov NDS a prípadných doplňujúcich pokynov NDS.
- e) vyhodnocovanie spôsobov riešenia KBI po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných KBI v súčinnosti s NDS,
- f) hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v prílohe č. 1 tejto Zmluvy a postupom a cez kontakty uvedené v prílohe č. 4 „Poriadku o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a. s. NDS“,
- g) samotný spôsob a forma hlásenia bezpečnostné incidentu sa bude riadiť platným predpisom NDS – „Poriadok o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a.s.“.
- h)

7. Bezpečnostné opatrenia- všeobecné

- i) Poskytovateľ/Zhotoviteľ je povinný poskytnúť súčinnosť NDS pri zabezpečovaní opatrení pre oblasť riadenia rizík a aktív, a to:
 - i) Odovzdanie evidencie aktív a komponentov vo formáte určenom NDS a aktualizácia evidencie aspoň raz do roka a poskytnutie aktuálnej evidencie na vyzvanie NDS,

- ii) Poskytnutie súčinnosti pri technickom vykonávaní kompletnej inventarizácie všetkých aktív v čase trvania zmluvy aspoň raz ročne na vyzvanie NDS, alebo v prípade rozsiahlej výmeny alebo modernizácie HW,
 - iii) Zabezpečiť pravidelnú údržbu a aktualizácie technických zariadení a softvérov v zmysle hlavného zmluvného vzťahu,
 - iv) Poskytovateľ/Zhotoviteľ musí prispôbiť opatrenia na základe spätnej väzby od NDS a výsledkov hodnotení rizík v súlade s postupmi pre zmenové požiadavky definovanými hlavnou zmluvou,
 - v) NDS s Poskytovateľom/Zhotoviteľom musí pravidelne revidovať a aktualizovať opatrenia na riadenie rizík a ochranu aktív v súlade so zmenami v prostredí a novými hrozbami.
- ii) Poskytovateľ/Zhotoviteľ je povinný zaviazat' svojich zamestnancov týmito povinnosťami:
- i) zamestnancovi Poskytovateľa/Zhotoviteľa sa zakazuje zverejňovať alebo inej osobe vyraziť svoje autentizačné údaje (heslá), taktiež sa zakazuje držanie záznamu hesiel (napr. na papieri, v softvérovom súbore, na prenosnom zariadení a pod),
 - ii) Zamestnanec Poskytovateľa/Zhotoviteľa je povinný chrániť pridelený autentizačný prostriedok pred odcudzením a zničením a nesmie ho prenechať inej osobe,
 - iii) zamestnancovi Poskytovateľa/Zhotoviteľa sa zakazuje pristupovať k IT aktívam, ktoré nie sú predmetom zmluvného vzťahu a vykonávať na nich akúkoľvek činnosť,
 - iv) zamestnancovi Poskytovateľa/Zhotoviteľa sa zakazuje vykonávať činnosti, ktoré nie sú predmetom zmluvného vzťahu.
 - v) Zamestnanec Poskytovateľa/Zhotoviteľa je povinný chrániť všetky informácie poskytnuté NDS pred ich únikom a zneužitím,

Príloha č. 3:**Záznam o kybernetickom bezpečnostnom incidente**

Záznam o kybernetickom bezpečnostnom incidente					
Názov bezpečnostného incidentu:				Číslo bezpečnostného incidentu:	(Vyplní NDS)
Dátum a čas vzniku bezpečnostného incidentu:			Dátum a čas hlásenia bezpečnostného incidentu:		
Bezpečnostný incident nahlásil:				Funkcia a osobné číslo:	
Útvar/úsek/spoločnosť:		Telefonický kontakt:		Email:	
Bezpečnostný incident zaevidoval:				Funkcia a osobné číslo:	
Dotknutá základná služba(príp. objekt) :					
Dotknuté IS a riadiace systémy:					
Popis incidentu:					
Dotknutý útvar:			Odhadovaný dopad:	Vyberte položku.	
Kategória bezpečnostného incidentu: (Vyplní NDS)	Vyberte položku.	Vstup/Spôsob hlásenia:	(Vyplní NDS)		
Hlásenie incidentu do JISKB NBÚ SR (Vyplní NDS)	Číslo: Forma hlásenia (rozhranie JISKB, email): Popis dotknutej základnej služby:				

Popis a vyčíslenie možného dopadu: (Vyplní NDS)			
Popis vyšetrovania incidentu: (Vyplní dodávateľ aj NDS)			
Druh bezpečnostného incidentu:	Vyberte položku. Iné (uviesť):	Typ bezpečnostné ho incidentu:	Vyberte položku. Iné (uviesť):
Popis prijatých/navrhovaných opatrení: (Vyplní dodávateľ aj NDS)			
Opatrenie:	Popis opatrenia:	Útvar/osoba zodpovedná za riešenie:	Termín splnenia:

Poznámky:	
Zoznam príloh:	
Podpisy zodpovedných osôb:	Hlásenie o KBI podal: Hlásenie o KBI prijal: Navrhované opatrenia schválil: